(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－91301
（P2002－91301A）
(43)公開日　平成14年３月27日(2002.3.27)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	

審査請求　未請求　請求項の数９　ＯＬ　（全 19 頁）

(21)出願番号　特願2000－284051(P2000－284051)

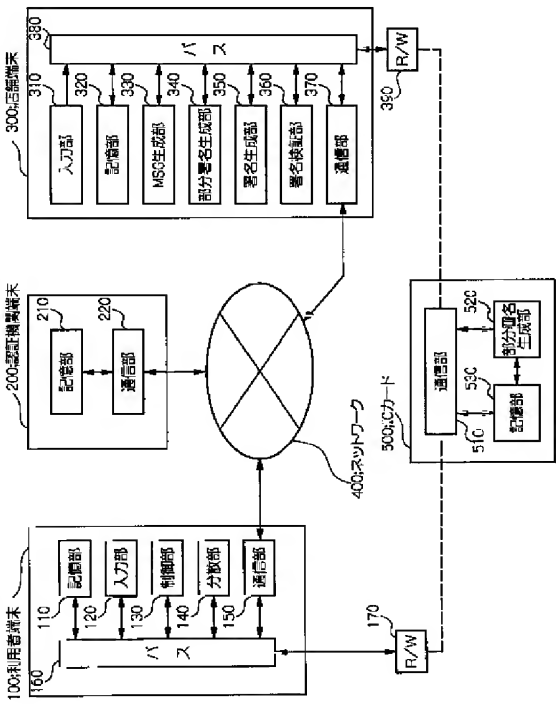
(22)出願日　平成12年９月19日(2000.9.19)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　佐藤　秀紀
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

Ｆターム(参考)　5J104 AA09 AA16 EA04 EA13 JA21
LA03 LA06 MA02 NA02 PA10

(54)【発明の名称】　鍵情報分散装置、演算装置および署名検証装置

(57)【要約】
【課題】　秘密鍵の紛失、盗難などが発生しても鍵情報の機密性の向上を図ることができる鍵情報分散端末、ＩＣカードおよび店舗端末を提供する。
【解決手段】　電子署名を生成するための鍵情報をｎ個（ｎは２以上の自然数）に分割し、分割した鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名を生成するための部分鍵情報を生成する分散手段と、所定のプログラムに基づいて電子署名を生成する演算装置に対し、前記分散手段によって生成される部分鍵情報のうち、ｋ個未満の部分鍵情報を格納する制御または、他の部分鍵情報のうちｋ個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段とを有することを特徴とする。



【特許請求の範囲】
【請求項１】　電子署名を生成するための鍵情報をｎ個（ｎは２以上の自然数）に分割し、分割した鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名を生成するための部分鍵情報を生成する分散手段と、
所定のプログラムに基づいて電子署名を生成する演算装置に対し、前記分散手段によって生成される部分鍵情報のうち、ｋ個未満の部分鍵情報を格納する制御または、他の部分鍵情報のうちｋ個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段と、
を有することを特徴とする鍵情報分散装置。
【請求項２】　前記電子署名を生成するための鍵情報をｎ個（ｎは２以上の自然数）に分割し、分割した鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報を生成する第１の分散手段と、
前記第１の分散手段が生成する第１の部分鍵情報のうち少なくとも１個の第１の鍵情報をさらにｍ個（ｍは２以上の自然数）に分割し、分割した鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報を生成する第２の分散手段と、
前記第２の分散手段によって生成される第２の部分鍵情報のうちｊ個未満の第２の部分鍵情報と前記第１の分散手段によって生成される第１の部分鍵情報のうち（ｋ－１）個の第１の部分鍵情報を電子署名を生成する演算装置に格納する制御または、
他の第２の部分鍵情報のうち、ｊ個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段と、
を有することを特徴とする鍵情報分散装置。
【請求項３】　電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、
前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名を生成するための部分鍵情報のうちｋ個未満の部分鍵情報を記憶する第１の記憶手段と、
前記署名検証装置から前記通信手段を介して送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第２の記憶手段と、
前記第１の記憶手段に記憶される部分鍵情報と前記第２の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、
前記通信手段によって前記部分署名生成手段によって生成される部分署名情報を前記署名検証装置に送信することを特徴とする演算装置。
【請求項４】　電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、
前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報のうちｋ個未満を記憶する第１の記憶手段と、
第１の部分鍵情報のうち少なくとも１個の第１の鍵情報がさらにｍ個（ｍは２以上の自然数）に分割され、分割された鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報のうちｊ個未満を記憶する第２の記憶手段と、
前記署名検証装置から送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第３の記憶手段と、
前記第２の記憶手段に記憶される第２の部分鍵情報と前記第３の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する第１の部分署名情報と合成することによって第２の部分署名情報が生成される情報となる部分署名情報を生成する部分署名生成手段と、
前記署名検証装置から送信される第２の部分署名情報と前記第１の記憶手段に記憶される第１の部分鍵情報とに基づいて、前記電子署名によって署名を行うための電子署名を生成する署名情報生成手段とを有し、
前記通信手段は、前記署名生成手段が生成する電子署名を前記署名検証装置に送信することを特徴とする演算装置。
【請求項５】　演算装置から送信される電子署名によって署名を行うための情報の通信を行い、電子署名を生成する署名検証装置において、
前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される部分鍵情報を記憶する第１の記憶手段と、
前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成手段と、
前記ＭＳＧ生成手段によって生成されるメッセージを記憶する第２の記憶手段と、
前記第１の記憶手段に記憶される部分鍵情報と前記第２の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段と、
前記演算装置から送信される部分署名情報と前記部分署名生成手段によって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成手段と、
を有することを特徴とする署名検証装置。
【請求項６】　所定のプログラムにより電子署名を生成する演算装置へ電子署名によって署名を行うための情報を送信し、前記演算装置から電子署名を受信する署名検

証装置において、
前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報のうち少なくとも１個の第１の鍵情報がをさらにｍ個（ｍは２以上の自然数）に分割され、分割された鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報のうちｊ個未満の第２の部分鍵情報を記憶する第１の記憶手段と、
前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成手段と、
前記ＭＳＧ生成手段によって生成されるメッセージを記憶する第２の記憶手段と、
前記第１の記憶手段に記憶される第２の部分鍵情報と前記第２の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算装置に記憶される第１の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成手段と、
を有することを特徴とする署名検証装置。
【請求項７】　電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、
前記電子署名によって署名を行う店舗を特定するための情報となる使用先コードと前記電子署名を生成するための部分鍵情報とを記憶する記憶手段と、
前記記憶手段に記憶される使用先コードを前記通信手段によって受信する電子署名を行う文書の内容に関する情報となるメッセージに付加するとともに、前記使用先コードが付加されたメッセージと前記記憶手段に記憶される部分鍵情報とに基づいて、前記署名検証装置によって生成される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、
前記通信手段は、前記部分署名生成手段が生成する部分署名を前記署名検証装置に送信することを特徴とする演算装置。
【請求項８】　演算装置から送信される署名を行うための情報に基づいて、電子署名を生成する電子署名生成プログラムを記憶したコンピュータ読みとり可能な記録媒体において、
前記電子署名生成プログラムは、
前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される部分鍵情報を記憶する記憶ステップと、
前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成ステップと、
前記ＭＳＧ生成ステップにおいて生成されるメッセージと、前記記憶ステップにおいて記憶される部分鍵情報とに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成ステップ
と、
前記演算装置から送信される部分署名情報と前記部分署名生成ステップによって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成ステップと、
をコンピュータに行わせることを特徴とする電子署名生成プログラムを記録した記録媒体。
【請求項９】　所定のプログラムにより電子署名を生成する演算装置へ署名を行うための情報を送信し、前記演算装置から電子署名を受信する電子署名プログラムを記憶したコンピュータ読みとり可能な記録媒体において、
前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報のうち少なくとも１個の第１の鍵情報をさらにｍ個（ｍは２以上の自然数）に分割され、分割された鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報のうちｊ個未満の第２の部分鍵情報を記憶する記憶ステップと、
前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成ステップと、
前記記憶ステップにおいて記憶される第２の部分鍵情報と前記ＭＳＧ生成ステップにおいて生成されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算装置に記憶される第１の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成ステップと、
をコンピュータに行わせることを特徴とする電子署名プログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、電子署名を生成するための秘密鍵の機密性を向上することができる鍵情報分散端末、ＩＣカードおよび店舗端末に関するものである。
【０００２】
【従来の技術】近年、印章の代わりに、ＩＣチップを搭載した記録媒体（以下、ＩＣカード）に署名用秘密鍵を書き込み、利用者は、このＩＣカードを携帯し、店等における商品の購入や契約時において、この秘密鍵を使用して電子署名を生成し、契約を成立させることが行われつつある。このＩＣカードの紛失、盗難が発生すると、悪意ある第三者に不正使用されるといった危険性がある。この危険を防止するために、以下に示す方法があった。
①ＩＣカードにＰＩＮ（個人識別番号）を設定する方法

パスワードや４桁の暗証番号であるＰＩＮをＩＣカードに設定し、このＰＩＮを入力すると、ＩＣカードに設定されている秘密鍵によって署名を行うことができるものである。

⑫ＣＲＬ（鍵廃棄リスト）を用いる方法。

ＩＣカードに設定された秘密鍵は、秘密鍵を利用する利用者の身分を証明するための証明書があり、この証明書は、認証機関によって管理されている。ＩＣカードの利用者は、ＩＣカードを紛失した場合にこの認証機関に連絡し、秘密鍵を無効にする届け出を行う。これにより、秘密鍵が無効になり、ＩＣカードの不正使用を防ぐことができる。

【０００３】

【発明が解決しようとする課題】しかしながら、上述した従来の方法においては、以下のような問題点があった。すなわち、⑪の方法においては、ＩＣカードの物理的なセキュリティが破られると、秘密鍵が読み出され、不正使用される可能性があった。さらに、ＩＣカードの使用毎にＰＩＮの入力をする必要があるため、カード使用者およびカード取り扱い店にとって手間がかかっていた。一方、⑫の方法においては、カード使用者がカードの紛失に気づいてから、ＩＣカードの秘密鍵を無効にする手続きを行うこととなるために、実際にカードを紛失してから利用者がカードの紛失に気づくまでの間と秘密鍵を無効にする手続きが完了するまでの間とがあるため、この間に悪意ある第三者に不正使用される可能性があった。さらに、⑫の方法においては、使用者の届け出によって秘密鍵を無効にした場合、ＩＣカードを使用するには、新たに認証機関に秘密鍵を使用するための手続きを行う必要があり、カード使用者にとってこの手続きが煩雑であった。

【０００４】本発明はこのような事情に鑑みてなされたもので、その目的は、秘密鍵の紛失、盗難などが発生しても鍵情報の機密性の向上を図ることができる鍵情報分散端末、ＩＣカードおよび店舗端末を提供することにある。

【０００５】

【課題を解決するための手段】上記目的を達成するために、本発明は、電子署名を生成するための鍵情報をｎ個（ｎは２以上の自然数）に分割し、分割した鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名を生成するための部分鍵情報を生成する分散手段と、所定のプログラムに基づいて電子署名を生成する演算装置に対し、前記分散手段によって生成される部分鍵情報のうち、ｋ個未満の部分鍵情報を格納する制御または、他の部分鍵情報のうちｋ個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段とを有することを特徴とする。

【０００６】また、本発明は、前記電子署名を生成するための鍵情報をｎ個（ｎは２以上の自然数）に分割し、分割した鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報を生成する第１の分散手段と、前記第１の分散手段が生成する第１の部分鍵情報のうち少なくとも１個の第１の鍵情報をさらにｍ個（ｍは２以上の自然数）に分割し、分割した鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報を生成する第２の分散手段と、前記第２の分散手段によって生成される第２の部分鍵情報のうちｊ個未満の第２の部分鍵情報と前記第１の分散手段によって生成される第１の部分鍵情報のうち（ｋ－１）個の第１の部分鍵情報を電子署名を生成する演算装置に格納する制御または、他の第２の部分鍵情報のうち、ｊ個未満の部分鍵情報を通信手段によって署名検証装置に送信する制御のうち少なくともいずれか一方の制御を行う制御手段とを有することを特徴とする。

【０００７】また、本発明は、電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名を生成するための部分鍵情報のうちｋ個未満の部分鍵情報を記憶する第１の記憶手段と、前記署名検証装置から前記通信手段を介して送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第２の記憶手段と、前記第１の記憶手段に記憶される部分鍵情報と前記第２の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、前記通信手段によって前記部分署名生成手段によって生成される部分署名情報を前記署名検証装置に送信することを特徴とする。

【０００８】また、本発明は、電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報のうちｋ個未満を記憶する第１の記憶手段と、第１の部分鍵情報のうち少なくとも１個の第１の鍵情報がさらにｍ個（ｍは２以上の自然数）に分割され、分割された鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報のうちｊ個未満を記憶する第２の記憶手段と、前記署名検証装置から送信される電子署名を行う文書の内容に関する情報となるメッセージを記憶する第３の記憶手段と、前記第２の記憶手段に記憶される第２の部分鍵情報と前記第３の記憶手段に記憶されるメッセージに基づいて、前記署名検証装置が有する第１の部

分署名情報と合成することによって第２の部分署名情報が生成される情報となる部分署名情報を生成する部分署名生成手段と、前記署名検証装置から送信される第２の部分署名情報と前記第１の記憶手段に記憶される第１の部分鍵情報とに基づいて、前記電子署名によって署名を行うための電子署名を生成する署名情報生成手段とを有し、前記通信手段は、前記署名生成手段が生成する電子署名を前記署名検証装置に送信することを特徴とする。

【０００９】また、本発明は、演算装置から送信される電子署名によって署名を行うための情報の通信を行い、電子署名を生成する署名検証装置において、前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される部分鍵情報を記憶する第１の記憶手段と、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成手段と、前記ＭＳＧ生成手段によって生成されるメッセージを記憶する第２の記憶手段と、前記第１の記憶手段に記憶される部分鍵情報と前記第２の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段と、前記演算装置から送信される部分署名情報と前記部分署名生成手段によって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成手段とを有することを特徴とする。

【００１０】また、本発明は、所定のプログラムにより電子署名を生成する演算装置へ電子署名によって署名を行うための情報を送信し、前記演算装置から電子署名を受信する署名検証装置において、前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報のうち少なくとも１個の第１の鍵情報がをさらにｍ個（ｍは２以上の自然数）に分割され、分割された鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報のうちｊ個未満の第２の部分鍵情報を記憶する第１の記憶手段と、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成手段と、前記ＭＳＧ生成手段によって生成されるメッセージを記憶する第２の記憶手段と、前記第１の記憶手段に記憶される第２の部分鍵情報と前記第２の記憶手段に記憶されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算装置に記憶される第１の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成手段とを有することを特徴とする。

【００１１】また、本発明は、電子署名を生成する署名検証装置に接続される通信手段を有する演算装置において、前記電子署名によって署名を行う店舗を特定するための情報となる使用先コードと前記電子署名を生成するための部分鍵情報とを記憶する記憶手段と、前記記憶手段に記憶される使用先コードを前記通信手段によって受信する電子署名を行う文書の内容に関する情報となるメッセージに付加するとともに、前記使用先コードが付加されたメッセージと前記記憶手段に記憶される部分鍵情報とに基づいて、前記署名検証装置によって生成される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成手段とを有し、前記通信手段は、前記部分署名生成手段が生成する部分署名を前記署名検証装置に送信することを特徴とする。

【００１２】また、本発明は、演算装置から送信される署名を行うための情報に基づいて、電子署名を生成する電子署名生成プログラムを記憶したコンピュータ読みとり可能な記録媒体において、前記電子署名生成プログラムは、前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される部分鍵情報を記憶する記憶ステップと、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成ステップと、前記ＭＳＧ生成ステップにおいて生成されるメッセージと、前記記憶ステップにおいて記憶される部分鍵情報とに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記電子署名が生成される情報となる部分署名情報を生成する部分署名生成ステップと、前記演算装置から送信される部分署名情報と前記部分署名生成ステップによって生成される部分署名情報に基づいて、前記電子署名を生成する署名生成ステップとをコンピュータに行わせることを特徴とする。

【００１３】また、本発明は、所定のプログラムにより電子署名を生成する演算装置へ署名を行うための情報を送信し、前記演算装置から電子署名を受信する電子署名プログラムを記憶したコンピュータ読みとり可能な記録媒体において、前記電子署名を生成するための鍵情報がｎ個（ｎは２以上の自然数）に分割され、分割された鍵情報をｋ個（ｋは１＜ｋ≦ｎとなる自然数）集めた場合に前記電子署名が生成される第１の部分鍵情報のうち少なくとも１個の第１の鍵情報がをさらにｍ個（ｍは２以上の自然数）に分割され、分割された鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に前記第１の部分鍵情報が生成される第２の部分鍵情報のうちｊ個未満の第２の部分鍵情報を記憶する記憶ステップと、前記電子署名を行う文書の内容に関する情報となるメッセージを生成するＭＳＧ生成ステップと、前記記憶ステップにおいて記憶される第２の部分鍵情報と前記ＭＳＧ生成ステップにおいて生成されるメッセージとに基づいて、前記演算装置から送信される部分署名情報と合成することによって前記演算

装置に記憶される第１の部分鍵情報と合成した場合に、前記電子署名が生成される部分署名情報を生成する部分署名生成ステップとをコンピュータに行わせることを特徴とする。

【００１４】

【発明の実施の形態】以下、本発明の一実施形態による鍵情報分散端末、ＩＣカードおよび店舗端末を図面を参照して説明する。ここでは、ＩＣカードを所有する利用者が、店舗に出向き、電子署名によって取引の契約を行う場合を例として説明する。図１は、この発明の一実施形態による電子署名システムの構成を示す概略ブロック図である。この図において、電子署名システムは、利用者端末１００と、認証機関端末２００と、店舗端末３００と、ネットワーク４００と、ＩＣカード５００とによって構成される。

【００１５】利用者端末１００は、記憶部１１０と、入力部１２０と、分散部１４０と、通信部１５０とがバス１６０によって接続され、装置各部間で各種データがバス１６０を介して制御部１３０の制御に基づいて送受信される。この利用者端末１００は、例えば、利用者の自宅に設けられる。

【００１６】制御部１３０は、分散部１４０に対し、秘密鍵ＳＫを所定の閾値ｋでｎ＋１個に分散する制御を行うとともに、バス１６０を介して各部のデータの転送を行う。ここで、秘密鍵ＳＫの分散について説明する。この秘密鍵ＳＫの分散は、シークレットシェアによって行われる。ここでいうシークレットシェアは、図２に示すように、秘密鍵ＳＫは、しきい値ｋでｎ個の部分秘密鍵ＳＫ１～ＳＫｎに分散される。そして、分散された部分秘密鍵ＳＫ１～ＳＫｎとメッセージとに基づいて、部分署名Ｓ１～Ｓｎが生成される。そして、部分署名Ｓ１～Ｓｎのうち、任意の部分署名Ｓｎがｋ個集まった場合に、署名Ｓが生成される。

【００１７】次に、図１に戻り、分散部１４０は、制御部１３０の指示に基づき、秘密鍵ＳＫを設定されるしきい値ｋ（＝２）で（ｎ＋１）個の部分秘密鍵を生成する。分散部１４０によって生成される部分秘密鍵は、１個の部分秘密鍵ＳＫａと、ｎ個の部分秘密鍵ＳＫｂ１～ＳＫｂｎとして出力される。記憶部１１０は、認証機関の公開鍵証明証において証明されている公開鍵ＰＫと秘密鍵ＳＫとの情報を記憶する。また、記憶部１１０は、分散部１４０が生成する部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ１～ＳＫｂｎを記憶する。また、記憶部１１０は、各種データを記憶する。

【００１８】通信部１５０は、ネットワーク４００を介して、認証機関端末２００および店舗端末３００と通信を行う。入力部１２０は、利用者端末１００を使用する利用者からの入力に応じた信号を出力する。さらに、利用者端末１００の外部には、ＩＣカード５００とバス１６０の間のデータの送受信を行う入出力装置（以下、「Ｒ／Ｗ」と称す）１７０が接続される。

【００１９】認証機関端末２００は、記憶部２１０と、通信部２２０とによって構成される。記憶部２１０は、利用者端末１００の利用者が所有する公開鍵ＰＫを記憶する。通信部２２０は、ネットワーク４００を介して利用者端末１００または店舗端末３００と通信を行い、必要に応じて利用者の公開鍵ＰＫの送受信を行う。この認証機関端末２００は、例えば、公開鍵を保管する認証機関に設けられる。

【００２０】店舗端末３００は、入力部３１０と、記憶部３２０と、ＭＳＧ生成部３３０と、部分署名生成部３４０と、署名生成部３５０と、署名検証部３６０と、通信部３７０と、バス３８０とによって構成される。店舗端末３００の各部は、バス３８０によって接続され、制御部によってデータの送受信が制御される。この店舗端末３００は、例えば、商品の販売店や、金融機関などの店舗ｉに設けられる（ただし、１≦ｉ≦ｎであり、ｎは、使用先となる店舗端末３００の数）。

【００２１】入力部３１０は、利用者から入力される指示に応じた信号を出力する。記憶部３２０は、公開鍵ＰＫ、部分秘密鍵ＳＫｂｉを記憶する。また、記憶部３２０は、各種データを記憶する。ＭＳＧ生成部３３０は、契約者となる利用者と契約を結ぶための契約書となるメッセージ（以下、「Ｍｓｇ」と称す）を生成する。部分署名生成部３４０は、部分秘密鍵ＳＫｂｎとＭｓｇとに基づいて、部分署名ＳＫｎを生成する。署名生成部３５０は、部分署名Ｓａ～Ｓｎがｋ個集まった場合に契約を成立させるための電子署名となる署名Ｓを生成する。

【００２２】署名検証部３６０は、署名生成部３４０が生成した署名Ｓと公開鍵ＰＫとに基づいて、署名Ｓが保証できるか否かを検証する。通信部３７０は、ネットワーク４００を介して利用者端末１００または認証機関端末２００と通信を行う。さらに、店舗端末３００の外部には、バス３８０とＩＣカード５００との間のデータの送受信を行うＲ／Ｗ３９０が接続される。

【００２３】次に、図３のフローチャートを用いて、図１の電子署名システムの動作について説明する。まず、利用者は、利用者端末１００によって公開鍵ＰＫと秘密鍵ＳＫを生成し、ネットワーク４００を介して公開鍵ＰＫを認証機関端末２００へ送信して登録するとともに、秘密鍵ＳＫを記憶部１１０に記憶する。一方、店舗ｉの店員は、店舗端末３００によって、ネットワーク４００を介して認証機関２００から利用者の公開鍵ＰＫを読み出して、記憶部３２０に記憶する（ステップＳ１）。次に、利用者は、入力部１２０から、秘密鍵ＳＫの分割の指示を入力する。入力部１２０から秘密鍵ＳＫの分割が指示されると、制御部１３０は、記憶部１１０から秘密鍵ＳＫを読み出して分散部１４０へ出力するとともに、しきい値２で（ｎ＋１）個に分割する指示を行う（ステップＳ２）。

【００２４】分割の指示を受けると、分散部１４０は、記憶部１１０から出力された秘密鍵ＳＫをしきい値２で（ｎ＋１）個に分割し、分割結果を部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ１～ＳＫｂｎとして記憶部１１０に記憶する（ステップＳ３）。部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ１～ＳＫｂｎが記憶部１１０に記憶された後、利用者によってＩＣカード５００がＲ／Ｗ１７０に挿入されると、制御部１３０は、記憶部１１０に記憶された部分秘密鍵ＳＫａを読み出し、バス１６０を介してＲ／Ｗ１７０に出力する。Ｒ／Ｗ１７０は、利用者端末１００から出力された部分秘密鍵ＳＫａをＩＣカード５００に出力する。ＩＣカード５００は、通信部５１０を介してＲ／Ｗ１７０から部分秘密鍵ＳＫａを受信すると、記憶部５３０に記憶する（ステップＳ４）。

【００２５】次に、利用者は、ＩＣカードを利用する店舗であって、利用者自身が部分秘密鍵ＳＫｂ１の管理を信頼できる店舗ｉを選択し、選択した店舗ｉの店舗端末３００に部分秘密鍵ＳＫｂｉを送信する指示を入力部１２０から入力する。入力部１２０から店舗端末３００に部分秘密鍵ＳＫｂｉを送信する指示が入力されると、制御部１３０は、バス１６０と通信部１５０とネットワーク４００を介して店舗端末３００の通信部３７０に部分秘密鍵ＳＫｂｉを送信する（ステップＳ５）。通信部３７０によって利用者端末１００から部分秘密鍵ＳＫｂｉを受信すると、受信した部分秘密鍵ＳＫｂｉを記憶部３２０に記憶し、利用者リストに登録する（ステップＳ６）。

【００２６】次に、利用者は、取引の契約を行う場合、ＩＣカード５００を携帯して、店舗端末３００が設置されている店舗ｉへ出向く。そして、利用者は、店舗端末３００の従業員に、取引の契約を行うための契約書の作成を依頼する。従業員は、契約を行うために必要な情報を入力部３１０から入力し、Ｍｓｇの生成を指示する。ＭＳＧ生成部３３０は、入力部３１０から入力された情報に基づいて、Ｍｓｇを生成し（ステップＳ８）、生成したＭｓｇを記憶部３２０に記憶する。

【００２７】次に、利用者と従業員との間で取引に関する交渉がなされた後、利用者が取引の契約をする場合、利用者は、ＩＣカード５００を店舗端末３００のＲ／Ｗ３９０に挿入する。ＩＣカード５００がＲ／Ｗ３９０に挿入された後、従業員によって入力部３１０からＭｓｇの転送が指示されると、記憶部３２０は、記憶しているＭｓｇをＲ／Ｗ３９０に出力する。Ｒ／Ｗ３９０は、店舗端末３００から出力されたＭｓｇを挿入されているＩＣカード５００の通信部５１０に転送する（ステップＳ９）。通信部５１０は、Ｒ／Ｗ３９０から転送されたＭｓｇを記憶部５３０に出力する。記憶部５３０は、通信部５１０から出力されたＭｓｇを記憶する。

【００２８】次に、部分署名生成部５２０は、記憶部５３０にＭｓｇが記憶されると、記憶されたＭｓｇと部分秘密鍵ＳＫａとを読み出し、読み出したＭｓｇと部分秘密鍵ＳＫａとに基づいて、部分署名Ｓａを生成する（ステップＳ１０）。そして、部分署名生成部５２０は、店舗端末３００に生成した部分署名生成部Ｓａを通信部５１０に出力する。通信部５１０は、部分署名生成部５２０から出力された部分署名生成部ＳａをＲ／Ｗ３９０を介して店舗端末３００に転送する（ステップＳ１１）。部分署名生成部Ｓａが送信されると、店舗端末３００の記憶部３２０は、ＩＣカード５００から転送された部分署名生成部Ｓａを記憶する（ステップＳ１２）。

【００２９】一方、店舗端末３００の部分署名生成部３４０は、ＩＣカードにＭｓｇの転送が完了すると、記憶部３２０に記憶されているＭｓｇと利用者の部分秘密鍵ＳＫｂｉとを読み出して、店舗ｉにおける部分署名Ｓｂｉを生成する（ステップＳ１３）。部分署名Ｓｂｉが生成されると、署名生成部３５０は、記憶部３２０に記憶されている部分署名生成部Ｓａを読み出し、この部分署名生成部Ｓａと部分署名生成部３４０によって生成された部分署名Ｓｂｉとに基づいて、署名Ｓを生成する（ステップＳ１４）。署名Ｓが生成されると、署名検証部３６０は、記憶部３２０から利用者の公開鍵ＰＫを読み出し、生成された署名Ｓを検証する（ステップＳ１５）。

【００３０】上記の実施形態において、利用者端末１００の入力部１２０から入力される利用者からの指示に応じて店舗端末３００に部分秘密鍵ＳＫｂ１～ＳＫｂｎのうち部分秘密鍵ＳＫｂｉを送信するようにしたので、利用者自身が部分秘密鍵ＳＫｂｎの管理を信頼できる店舗を選択して送信することができる。これにより、いずれかの部分秘密鍵ＳＫｂ１～ＳＫｂｎを有していない店舗において、ＩＣカード５００を利用することができないので、ＩＣカード５００の使用範囲を限定でき、これにより、ＩＣカード５００の盗難、部分秘密鍵ＳＫａの情報が盗まされた場合において、部分秘密鍵ＳＫａが第三者に悪用される可能性を低減させることができる効果が得られる。

【００３１】次に、この発明の第２の実施形態について、図面を用いて説明する。図４は、第２の実施形態における電子署名システムの構成を示す概略ブロック図である。同図において図１の各部に対応する部分には同一の符号を付け、その説明を省略する。利用者端末１００の分散部１４１は、秘密鍵ＳＫを部分秘密鍵ＳＫａと部分秘密鍵ＳＫｂとに分割する。また、分散部１４１は、部分秘密鍵ＳＫｂを制御部１３０からの指示に基づき、しきい値ｋ（＝２）で（ｎ＋１）個の部分秘密鍵を生成する。分散部１４１によって生成される部分秘密鍵は、１個の部分秘密鍵ＳＫｂ０と、ｎ個の部分秘密鍵ＳＫｂ１～ＳＫｂｎとして出力される。

【００３２】店舗端末３００の署名生成部３５１は、部分署名Ｓｂｉと部分署名Ｓｂ０とに基づいて部分署名Ｓｂを生成し、生成した部分署名ＳｂをＩＣカード５００

に送信する指示をする。ＩＣカード５００の署名生成部５４０は、部分署名Ｓｂと部分秘密鍵ＳＫａとに基づいて、署名Ｓを生成する。

【００３３】次に、図４の構成における装置各部の動作について、図５のフローチャートを用いて説明する。まず、図１のステップＳ１の処理と同様に、利用者端末１００によって公開鍵ＰＫが認証機関端末２００に登録され、秘密鍵ＳＫが記憶部１１０に記憶されるとともに、店舗端末３００によって、認証機関２００から利用者の公開鍵ＰＫが読み出され、記憶部３２０に記憶される（ステップＳ５１）。

【００３４】次に、利用者は、入力部１２０から、秘密鍵ＳＫの分割の指示を入力する。入力部１２０から秘密鍵ＳＫの分割が指示されると、制御部１３０は、記憶部１１０から秘密鍵ＳＫを読み出して分散部１４１へ出力するとともに、しきい値２で（ｎ＋１）個に分割する指示を行う。

【００３５】分割の指示を受けると、分散部１４１は、まず、記憶部１１０から出力された秘密鍵ＳＫを部分秘密鍵ＳＫａと部分秘密鍵ＳＫｂとに分割し（ステップＳ５２）、部分秘密鍵ＳＫａを記憶部１１０に記憶する。次いで、分散部１４１は、制御部１３０からの指示に基づき、部分秘密鍵ＳＫｂをしきい値２で（ｎ＋１）個に分割し（ステップＳ５３）、分割結果を部分秘密鍵ＳＫｂ０～ＳＫｂｎとして記憶部１１０に記憶する。部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ０～ＳＫｂｎが記憶部１１０に記憶された後、利用者によってＩＣカード５００がＲ／Ｗ１７０に挿入されると、制御部１３０は、記憶部１１０に記憶された部分秘密鍵ＳＫａと部分秘密鍵ＳＫｂ０とを読み出し、バス１６０とＲ／Ｗ１７０を介して、ＩＣカード５００に出力する。ＩＣカード５００は、通信部５１０を介してＲ／Ｗ１７０から部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ０を受信すると、記憶部５３０に記憶する（ステップＳ５４）。

【００３６】次に、利用者は、ＩＣカードを利用する店舗であって、利用者自身が部分秘密鍵ＳＫｂｎの管理を信頼できる店舗ｉを選択し、選択した店舗ｉの店舗端末３００に部分秘密鍵ＳＫｂｉを送信する指示を入力部１２０から入力する。入力部１２０から店舗端末３００に部分秘密鍵ＳＫｂｉを送信する指示が入力されると、制御部１３０は、バス１６０と通信部１５０とネットワーク４００を介して店舗端末３００の通信部３７０に部分秘密鍵ＳＫｂｉを送信する（ステップＳ５５）。通信部３７０によって利用者端末１００から部分秘密鍵ＳＫｂｉを受信すると、受信した部分秘密鍵ＳＫｂｉを記憶部３２０に記憶し、利用者リストに登録する（ステップＳ５６）。

【００３７】次に、利用者は、第１の実施形態と同様に、ＩＣカード５００を携帯して、店舗端末３００が設置されている店舗ｉへ出向き、契約書の作成を依頼する。従業員は、店舗端末３００によって署名対象となるＭｓｇを生成し（ステップＳ５６）、生成したＭｓｇを記憶部３２０に記憶する。

【００３８】次に、利用者と従業員との間で取引に関する交渉がなされた後、利用者が取引の契約をする場合、利用者によってＩＣカード５００がＲ／Ｗ３９０に挿入された後、従業員によって入力部３１０からＭｓｇの転送が指示されると、記憶部３２０は、記憶しているＭｓｇをＲ／Ｗ３９０に出力する。Ｒ／Ｗ３９０は、店舗端末３００から出力されたＭｓｇを挿入されているＩＣカード５００の通信部５１０に転送する（ステップＳ５９）。通信部５１０は、Ｒ／Ｗ３９０から転送されたＭｓｇを記憶部５３０に出力する。記憶部５３０は、通信部５１０から出力されたＭｓｇを記憶する。

【００３９】次に、部分署名生成部５２０は、記憶部５３０にＭｓｇが記憶されると、記憶部５３０から記憶されたＭｓｇと部分秘密鍵ＳＫｂ０とを読み出し、読み出したＭｓｇと部分秘密鍵ＳＫｂ０とに基づいて、部分署名Ｓｂ０を生成する（ステップＳ６０）。そして、部分署名生成部５２０は、生成した部分署名生成部Ｓｂ０を通信部５１０に出力する。通信部５１０は、部分署名生成部５２０から出力された部分署名生成部ＳａをＲ／Ｗ３９０を介して店舗端末３００に転送する（ステップＳ６１）。部分署名生成部Ｓａが送信されると、店舗端末３００の記憶部３２０は、ＩＣカード５００から転送された部分署名生成部Ｓｂ０を記憶する（ステップＳ６２）。

【００４０】一方、店舗端末３００の部分署名生成部３４０は、ＩＣカードにＭｓｇの転送が完了した後、記憶部３２０に記憶されているＭｓｇと利用者の部分秘密鍵ＳＫｂｉとを読み出して、店舗ｉにおける部分署名Ｓｂｉを生成する（ステップＳ６３）。部分署名Ｓｂｉが生成されると、署名生成部３５１は、記憶部３２０に記憶されている部分署名生成部Ｓｂ０を読み出し、この部分署名生成部Ｓｂ０と部分署名生成部３４０によって生成された部分署名Ｓｂｉとに基づいて、部分署名Ｓｂを生成し（ステップＳ６４）、Ｒ／Ｗ３９０に対し、生成した部分署名ＳｂをＩＣカード５００に送信する指示を行う。

【００４１】Ｒ／Ｗ３９０は、署名生成部３５１からの指示を受けて、部分署名ＳｂをＩＣカード５００に転送する（ステップＳ６５）。部分署名Ｓｂが転送されると、ＩＣカード５００の通信部５１０は、転送された部分署名Ｓｂを記憶部５３０に出力し、記憶する。部分署名Ｓｂが記憶部５３０に記憶されると、署名生成部５４０は、記憶部５３０に記憶されている部分署名Ｓｂと秘密鍵ＳＫａとを読み出し、署名Ｓを生成する（ステップＳ６６）。そして、署名生成部５４０は、生成した署名Ｓを記憶部５３０に記憶した後、通信部５１０によって店舗端末３００に送信する指示を行う。通信部５１０

は、署名生成部５４０からの指示を受けて、署名ＳをＲ／Ｗ３９０を介して店舗端末３００に送信する（ステップＳ６７）。

【００４２】店舗端末３００の記憶部３２０は、Ｒ／Ｗ３９０を介してＩＣカード５００から送信された署名Ｓを記憶する（ステップＳ６８）。署名Ｓが記憶された後、署名検証部３６０は、記憶部３２０から署名Ｓと利用者の公開鍵ＰＫを読み出し、公開鍵ＰＫによって署名Ｓの検証を行う（ステップＳ６９）。

【００４３】上述の実施形態においては、秘密鍵ＳＫを部分秘密鍵ＳＫａと部分秘密鍵ＳＫｂとに分割した後、部分秘密鍵ＳＫｂをさらに、部分秘密鍵ＳＫｂ０～部分秘密鍵ＳＫｂｎに分割し、部分秘密鍵ＳＫａと部分秘密鍵ＳＫｂ０とをＩＣカード５００に記憶し、部分秘密鍵ＳＫｂ１～部分秘密鍵ＳＫｂｎをそれぞれ店舗に送信するようにした。これにより、店舗同士が結託し、部分秘密鍵ＳＫｂｎを２つ集めた場合においても、部分秘密鍵ＳＫｂしか生成できないすなわち、秘密鍵ＳＫを生成することが不可能であるので、署名Ｓを生成して不正使用することを防ぐことが可能である。なお、上述の実施形態において、秘密鍵ＳＫを部分秘密鍵ＳＫａと部分秘密鍵ＳＫｂとに分割したが、秘密鍵ＳＫをｍ個（ｍは２以上の自然数）に分割し、分割した鍵情報をｊ個（１＜ｊ≦ｍ）集めた場合に第１の部分鍵情報が生成されるようにしてもよい。

【００４４】次に、この発明の第３の実施形態について図面を用いて説明する。図６は、第３の実施形態における電子署名システムの構成を示す概略ブロック図である。この図において、図１の各部に対応する部分には、同一の符号を付け、その説明を省略する。利用者端末１００の制御部１３１は、図１の制御部１３０の機能にさらに、乱数生成部１８０に乱数の生成を指示する機能を有し、利用者端末１００の各部の動作を制御する。乱数生成部１８０は、制御部１３０からの指示に基づいて、乱数を生成する。

【００４５】部分秘密鍵演算部１９０は、部分秘密鍵ＳＫｂと乱数Ｒとｆ（ｉ）とに基づいて、以下に示す（１）式を用いて部分秘密鍵ＳＫｂｉを演算する。

ＳＫｂ＋Ｈ（ｆ（ｉ）‖Ｒ）　……（１）

ただし、Ｈ（ｆ（ｉ）‖Ｒ）はハッシュ関数によって計算をおこなうものである。ｆ（ｉ）は、ユニークコードであり、店舗に設置された店舗端末３００毎に異なる値が設定される。このユニークコードｆ（ｉ）は、例えば、利用者によって任意に決定される値であり、例えば、利用者に関する情報、利用する店舗ｉの店の名前、電話番号、住所などの情報に基づいて決定される。

【００４６】ＩＣカード５００の部分秘密鍵演算部５５０は、部分秘密鍵ＳＫａと乱数Ｒとユニークコードｆ（ｉ）とに基づいて、以下に示す（２）式を用いて部分秘密鍵ＳＫａｉを演算する。

ＳＫａ－Ｈ（ｆ（ｉ）‖Ｒ）　……（２）

【００４７】部分署名生成部５２０は、Ｍｓｇと部分秘密鍵ＳＫａｉとに基づいて、以下に示す（３）式を用いて部分署名Ｓａを生成する。

$Sa=MSG^{SKai} \bmod (n)$　……（３）

部分署名生成部３４０は、Ｍｓｇと部分秘密鍵ＳＫｂｉとに基づいて、以下に示す（４）式を用いて部分署名Ｓｂを生成する。

$Sb=MSG^{SKbi} \bmod (n)$　……（４）

【００４８】署名生成部３５０は、部分署名Ｓａと部分署名Ｓｂとに基づいて、以下に示す（５）式を用いて、署名Ｓを生成する。

$S=Sai \times Sbi \bmod (n)$　……（５）

【００４９】次に、図６の構成における装置の動作について図７および図８のフローチャートを用いて説明する。図７は、図６の構成における装置の動作を説明するフローチャート、図８は、部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂｉをＩＣカード５００、店舗端末３００に設定する動作を説明するためのフローチャートである。

【００５０】まず、図７のフローチャートを用いて図６の構成における装置の動作について説明する。利用者端末１００によって公開鍵ＰＫが認証機関端末２００に登録され、秘密鍵ＳＫが記憶部１１０に記憶されるとともに、店舗端末３００によって、認証機関２００から利用者の公開鍵ＰＫが読み出され、記憶部３２０に記憶される。

【００５１】次に、利用者は、入力部１２０から、ユニークコードｆ（ｉ）を入力するとともに、秘密鍵ＳＫの分割の指示を入力する。入力部１２０から秘密鍵ＳＫの分割が指示されると、制御部１３１は、ユニークコードｆ（ｉ）を記憶部１１０に記憶するとともに、秘密鍵ＳＫを分割し、分割した部分秘密鍵をＩＣカード５００と、店舗端末３００に設定する制御を行う（ステップＳ１０１）。ここで、ステップＳ１０１における装置の動作について図８のフローチャートを用いて説明する。

【００５２】まず、制御部１３１は、乱数生成部１８０に乱数を生成する指示を行う。乱数生成部１８０は、制御部１３１からの指示に基づいて、乱数Ｒを生成し（ステップＳ２０１）、生成した乱数Ｒを記憶部１１０に出力し、記憶部１１０に記憶する（ステップＳ２０２）。次に、制御部１３１は、分散部１４０に、秘密鍵ＳＫを分割する指示を行う。分散部１４０は、制御部１３１からの指示に基づいて、秘密鍵ＳＫを２つに分割し（ステップＳ２０３）、部分秘密鍵ＳＫａと部分秘密鍵ＳＫｂとして記憶部１１０に記憶する（ステップＳ２０４）。

【００５３】記憶部１１０に部分秘密鍵ＳＫａが記憶された後、利用者によってＩＣカード５００がＲ／Ｗ１７０に挿入されると、制御部１３１は、記憶部１１０から部分秘密鍵ＳＫａと乱数Ｒを読み出し、バス１６０とＲ／Ｗ１７０とを介してＩＣカード５００に転送する制御

を行う。ＩＣカード５００の通信部５１０は、Ｒ／Ｗから出力される部分秘密鍵ＳＫａと乱数Ｒを受信すると、受信した部分秘密鍵ＳＫａと乱数Ｒを記憶部５３０に記憶する（ステップＳ２０５）。

【００５４】さらに、制御部１３１は、記憶部１１０から部分秘密鍵ＳＫｂと乱数ＲとユニークコードＦ（ｉ）を読み出し、部分秘密秘密鍵演算部１９０に出力するとともに、部分秘密鍵ＳＫｂｉを生成する指示をする。部分秘密秘密鍵演算部１９０は、（１）式と、部分秘密鍵ＳＫｂと乱数ＲとユニークコードＦ（ｉ）に基づいて部分秘密鍵ＳＫｂｉを生成し（ステップＳ２０５）、生成した部分秘密鍵ＳＫｂｉを通信部１５０に出力し、店舗端末３００に送信する指示をする。通信部１５０は、部分秘密秘密鍵演算部１９０からの指示に基づき、ネットワーク４００を介して店舗端末３００に送信する（ステップＳ２０６）。店舗端末３００の通信部３７０は、ネットワーク４００を介して利用者端末１００から受信した部分秘密鍵ＳＫｂｉを受信し（ステップＳ２０７）、記憶部３２０に出力する。記憶部３２０は、通信部３７０から出力された部分秘密鍵ＳＫｂｉを記憶する（ステップＳ２０８）。

【００５５】次に、図７に戻り、ＩＣカード５００に部分秘密鍵ＳＫａｉが記憶され（ステップＳ）、店舗端末３００に部分秘密鍵ＳＫｂｉが記憶された後（ステップＳ１０３）、利用者は、ＩＣカード５００を携帯して、店舗端末３００が設置されている店舗ｉへ出向き、従業員との間で取引に関する交渉を行う。そして、利用者と従業員との間で取引に関する交渉がなされた後、利用者が取引の契約をする場合、利用者によってＩＣカード５００がＲ／Ｗ３９０に挿入された後、利用者は、ユニークコードＦ（ｉ）を店舗端末３００の入力部３１０から入力する（ステップＳ１０３）。入力部３１０から入力されたユニークコードＦ（ｉ）は、バス３８０とＲ／Ｗ３９０を介してＩＣカード５００に出力される。そして、ＩＣカード５００の通信部５１０入力よってユニークコードＦ（ｉ）が受信され（ステップＳ１０４）、記憶部５３０に出力され、記憶される。

【００５６】次に、店舗ｉの従業員からＭｓｇの生成が指示されると、ＭＳＧ生成部３３０によって署名対象となるＭｓｇが生成され（ステップＳ１０５）、生成されたＭｓｇが記憶部３２０に記憶されるとともに、Ｒ／Ｗ３９０を介してＩＣカード５００に送信される（ステップＳ１０６）。ＩＣカード５００の通信部５１０は、Ｍｓｇを受信し（ステップＳ１０７）、Ｍｓｇを記憶部５３０に出力し、記憶する。Ｍｓｇが記憶部５３０に記憶されると、部分秘密鍵生成部５５０は、記憶部５３０に記憶されている部分秘密鍵ＳＫａとユニークコードＦ（ｉ）と乱数Ｒに基づいて、上記（２）式によって、部分秘密鍵ＳＫａｉを生成する（ステップＳ１０８）。そして、部分秘密鍵生成部５５０は、生成した部分秘密鍵ＳＫａｉを記憶部５３０に記憶する。

【００５７】部分秘密鍵ＳＫａｉが記憶部５３０に記憶されると、部分署名生成部５２０は、記憶部５３０に記憶された部分秘密鍵ＳＫａｉとＭｓｇに基づいて、上記（３）式を用いて、部分署名Ｓａを生成し（ステップＳ１０９）、記憶部５３０に記憶する。記憶部５３０に部分署名Ｓａが記憶されると、通信部５１０は、記憶部５３０から部分署名Ｓａを読み出して、Ｒ／Ｗ３９０を介して店舗端末３００に送信する（ステップＳ１１０）。

【００５８】一方、店舗端末３００の部分署名生成部３４０は、部分秘密鍵ＳＫｂｉとＭｓｇを記憶部５３０から読み出して、上記（４）式を用いて、部分署名Ｓｂを生成し（ステップＳ１１１）、記憶部５３０に記憶する。次に、Ｒ／Ｗ３９０を介してＩＣカード５００から部分署名Ｓａを受信すると（ステップＳ１１２）、記憶部３２０は、部分署名Ｓａを記憶する。部分署名Ｓａが記憶部３２０に記憶されると、署名生成部３５０は、記憶部３２０に記憶された部分署名Ｓａと部分署名Ｓｂとを読み出して、上記（５）式を用いて署名Ｓを生成する（ステップＳ１１３）。署名Ｓが生成されると、署名Ｓが記憶部３２０に格納された後、署名検証部３６０によって、署名Ｓと利用者の公開鍵ＰＫとが記憶部３２０が読み出され、署名Ｓが公開鍵ＰＫによって検証される（ステップＳ１１４）。

【００５９】なお、上述した第３の実施形態において、ユニークコードＦ（ｉ）は、利用者だけが知り得る値であってもよく、店舗ｉが知り得る値であってもよい。また、ユニークコードＦ（ｉ）は、すべての店舗ｉにおいて共通する値であってもよい。

【００６０】次に、第４の実施形態について説明する。この実施形態においては、ユニークコードＦ（ｉ）をＭｓｇに設定する場合について図面を用いて説明する。図９は、第４の実施形態における電子署名システムの構成を示す概略ブロック図である。この図にいて、図６の各部に対応する部分には同一の符号を付け、その説明を省略する。この実施形態において、ユニークコードＦ（ｉ）は、使用先コードＩＤｉが設定される。この使用先コードＩＤｉは、使用先の店舗ｉの固有の情報に基づいて決定される値であり、例えば、店舗ｉの名称のデータが用いられる。

【００６１】次に、部分秘密鍵演算部１９０は、部分秘密鍵ＳＫｂと乱数Ｒとｆ（ｉ）とに基づいて、上述の（１）式を用いて部分秘密鍵ＳＫｂｉを演算するが、この実施形態において、ユニークコードＦ（ｉ）が使用先コードＩＤｉとなるので、以下に示す（６）に基づいて、部分秘密鍵ＳＫｂｉを演算する。

ＳＫｂ＋Ｈ（ＩＤｉ‖Ｒ）　……（６）

【００６２】ＩＣカード５００の部分秘密鍵演算部５５０は、部分秘密鍵ＳＫａと乱数ＲとユニークコードＦ（ｉ）とに基づいて、上述の（２）式を用いて部分秘密

鍵ＳＫａｉを演算するが、この実施形態において、ユニークコードｆ（ｉ）が使用先コードＩＤｉとなるので、以下に示す（７）に基づいて、部分秘密鍵ＳＫａｉを演算する。

ＳＫａ－Ｈ（ＩＤｉ‖Ｒ）　……（７）

【００６３】部分署名生成部５２１は、部分署名生成部５２０の機能においてさらに、記憶部５３０から使用先コードＩＤｉを読み出し、Ｍｓｇに使用先コードＩＤｉを付加して部分署名Ｓａを生成する。この部分署名生成部５２１は、以下に示す（８）式に基づいて部分署名Ｓａを生成する。

Ｓａ＝ＩＤｉ・ＭＳＧ^{SKai}ｍｏｄ（ｎ）　……（８）

部分署名生成部３４１は、部分署名生成部３４０の機能においてさらに、記憶部３２０から使用先コードＩＤｉを読み出し、Ｍｓｇに使用先コードＩＤｉを付加して部分署名Ｓｂを生成する。この部分署名生成部３４１は、以下に示す（９）式に基づいて部分署名Ｓｂを生成する。

Ｓｂ＝ＩＤｉ・ＭＳＧ^{SKbi}ｍｏｄ（ｎ）　……（９）

このような構成において、装置の各部は、図7と図8とにおける説明と同様に動作する。このように、Ｍｓｇに使用先コードＩＤｉを付加して部分署名Ｓａ、部分署名Ｓｂが生成され、この部分署名Ｓａと部分署名Ｓｂとに基づいて、署名生成部３５０によって署名Ｓが生成されると、図１０符号６００に示すように、使用先コードＩＤｉに関する情報がＭｓｇ（符号６１０）内に設定される。これにより、利用者は、部分秘密鍵ＳＫｂｉの送信となる店舗ｉでしか生成できないＭｓｇに対して電子署名を行うことが可能である。従って、第三者によって電子署名（符号６３０）が設定された契約書内の契約先の名称（符号６２０）が、利用者が実際には契約を行っていない場合の契約先の名称に改竄された場合、改竄された契約先名称とＭｓｇに予め設定されている契約先の名称（符号６００）とが異なるので、改竄を発見することが可能であり、署名Ｓを部分秘密鍵ＳＫｂｉの預け先以外に流用されることを防ぐことが可能である。

【００６４】なお、上述した第３の実施形態と第４の実施形態において、ユニークコードｆ（ｉ）は、店舗端末３００に部分秘密鍵ＳＫｂを送信するときに同時に送信するようにしてもよい。

【００６５】次に、第５の実施形態について図面を用いて説明する。図１１は、第５の実施形態における電子署名システムの構成について説明するための概略ブロック図である。この実施形態では、しきい値ｋを３に設定して、部分秘密鍵を利用者端末１００とＩＣカード５００と店舗端末３００に設定する場合を一例として説明する。図１１において、図９の各部に対応する部分には同一の符号を付け、その説明を省略する。部分署名生成部１９５は、記憶部１１０から使用先コードＩＤｉを読み出し、Ｍｓｇに使用先コードＩＤｉを付加して部分署名Ｓｃを生成する。この部分署名生成部１９５は、以下に示す（１０）式に基づいて部分署名Ｓｃを生成する。

Ｓｃ＝ＩＤｉ・ＭＳＧ^{SKci}ｍｏｄ（ｎ）　……（１０）

【００６６】次に、図１１の構成における装置の動作について、図面を用いて説明する。図１２は、図１１の構成における装置の動作について説明するためのフローチャートである。まず、図１のステップＳ１の処理と同様に、利用者端末１００によって公開鍵ＰＫが認証機関端末２００に登録され、秘密鍵ＳＫが記憶部１１０に記憶されるとともに、店舗端末３００によって、認証機関２００から利用者の公開鍵ＰＫが読み出され、記憶部３２０に記憶される。また、従業員によって設定される使用先コードＩＤｉが記憶部３２０に記憶される。次に、利用者は、入力部１２０から、入力部１２０から秘密鍵ＳＫの分割が指示されると、制御部１３０は、記憶部１１０から秘密鍵ＳＫを読み出して分散部１４０へ出力するとともに、しきい値３で３個に分割する指示を行う。さらに、制御部１３１は、乱数生成部１８０に乱数の生成を指示する。

【００６７】分散部１４０は、制御部１３１からの指示を受けて、秘密鍵ＳＫを３つに分割し、部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ、部分秘密鍵ＳＫｃを生成する（ステップＳ３０１）。そして、分散部１４０は、生成した部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ、部分秘密鍵ＳＫｃを記憶部１１０に記憶する（ステップＳ３０２）。

【００６８】一方、乱数生成部１８０は、制御部１３１からの指示に基づいて、乱数Ｒを生成し、記憶部１１０に記憶する。次に、制御部１３１は、記憶部１１０に記憶された部分秘密鍵ＳＫａと乱数Ｒを読み出し、Ｒ／Ｗ１７０を介してＩＣカード５００に送信する（ステップＳ３０３）。ＩＣカード５００の通信部５１０は、利用者端末１００から送信された部分秘密鍵ＳＫａと乱数Ｒとを受信し、記憶部５３０に記憶する（ステップＳ３０４）。

【００６９】次に、制御部１３１は、記憶部１１０から部分秘密鍵ＳＫｂと乱数ＲとＩＤｉを読み出して、部分秘密鍵演算部１９０に出力するとともに、部分秘密鍵ＳＫｂｉを生成する指示をする。部分秘密鍵演算部１９０は、制御部１３１からの指示に基づいて、部分秘密鍵ＳＫｂｉを生成し、記憶部１１０に記憶した後、通信部１５０とネットワーク４００を介して、店舗端末３００に送信する（ステップＳ３０５）。店舗端末３００の通信部３７０は、部分秘密鍵ＳＫｂｉを受信すると、記憶部３２０に記憶する（ステップＳ３０６）。

【００７０】次に、利用者は、ＩＣカード５００を携帯するとともに、利用者端末１００をネットワーク４００を介して通信可能な状態に設定しておき、店舗ｉに出向く。そして、利用者は、従業員と交渉を行い、契約を行う場合、従業員に契約書となるＭｓｇの生成を依頼す

る。従業員は、店舗端末３００によってＭｓｇ生成し、生成されるＭｓｇと使用先コードＩＤｉとを利用者端末１００に送信する指示を行う。

【００７１】店舗端末３００のＭＳＧ生成部３３０は、入力部１２０から入力される従業員からの指示に応じて、Ｍｓｇを生成し、生成したＭｓｇを記憶部３２０に記憶するとともに、通信部３７０とネットワーク４００を介して利用者端末１００に送信する。このとき、入力部３１０から入力される使用先コードＩＤｉの送信指示に応じて、記憶部３２０から使用先コードＩＤｉが読み出され、上記Ｍｓｇと同様に、利用者端末１００に送信される（ステップＳ３０８）。

【００７２】次に、店舗端末３００からＭｓｇと使用先コードＩＤｉが送信されると、通信部１５０は、Ｍｓｇと使用先コードＩＤｉとを受信して記憶部１１０に記憶する（ステップＳ３０９）。Ｍｓｇと使用先コードＩＤｉが記憶部１１０に記憶されると、部分署名生成部１９５は、記憶部１１０からＭｓｇ、部分秘密鍵ＳＫｃ、使用先コードＩＤｉを読み出し、これらに基づいて、使用先コードＩＤｉをＭｓｇに付加して部分署名Ｓｃを生成する。生成された部分署名Ｓｃは、通信部１５０によって、ネットワーク４００を介して店舗端末３００に送信される（ステップＳ３１１）。

【００７３】店舗端末３００において、通信部３７０は、部分署名Ｓｃを受信すると、記憶部３２０に記憶する（ステップＳ３１２）。そして、利用者によってＩＣカード５００がＲ／Ｗ３９０に挿入されると、記憶部３２０に記憶されているＭｓｇと使用先コードＩＤｉが読み出され、ＩＣカード５００に送信される（ステップＳ３１３）。ＩＣカード５００の通信部５１０は、受信したＭｓｇと使用先コードＩＤｉを記憶部５３０に出力して記憶する（ステップＳ３１４）。Ｍｓｇと使用先コードＩＤｉが記憶されると、部分秘密鍵生成部５５０は、部分秘密鍵ＳＫａと乱数Ｒと使用先コードＩＤｉとに基づいて、部分秘密鍵ＳＫａｉを生成し（ステップＳ３１５）、記憶部５３０に記憶する。部分秘密鍵ＳＫａｉが生成されると、部分署名生成部５２１は、Ｍｓｇに使用先コードＩＤｉを付加して部分秘密鍵ＳＫａｉを用いて部分署名Ｓａを生成し（ステップＳ３１６）、通信部５１０とＲ／Ｗ３９０を介して店舗端末３００に送信するとともに（ステップＳ３１７）、記憶部５３０に記憶する。

【００７４】店舗端末３００において部分署名Ｓａを受信すると（ステップＳ３１８）、受信した部分署名Ｓａを記憶部３２０に記憶する。部分署名Ｓａを受信した後、部分署名生成部３４１は、部分秘密鍵ＳＫｂｉと乱数Ｒと使用先コードＩＤｉを記憶部３２０から読みだし、部分署名Ｓｂを生成する（ステップＳ３１９）。部分署名Ｓｂが生成されると、署名生成部３５０は、部分署名Ｓａ、Ｓｂ、Ｓｃから署名Ｓを生成し（ステップＳ３２０）、生成した署名Ｓを記憶部３２０に記憶する。署名検証部３６０は、記憶部３２０から利用者の公開鍵ＰＫを読み出し、公開鍵ＰＫによって生成された署名Ｓを検証する（ステップＳ３２１）。

【００７５】なお、第５の実施形態において、秘密鍵ＳＫ、部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂ、部分秘密鍵ＳＫｃ、乱数Ｒを利用者端末１００、ＩＣカード５００以外の記録媒体に記録し、バックアップ用として保管してもよい。

【００７６】また、上記実施形態において、利用者端末１００にアクセスがある毎にログにアクセスの履歴を記憶するようにしてもよい。これにより、利用者がＩＣカードを紛失したり、ＩＣカードの部分秘密鍵がコピーされ、拾得者や悪意ある第３者がＩＣカードを不正使用しようとした場合においても利用者端末１００にアクセスの履歴が記録される。従って、利用者ＩＣカードの所有者である利用者は、不正使用されることを把握でき、利用者端末１００を停止させることによって、以後の不正使用を防止することが可能である。また、利用者端末１００に記録されたアクセス履歴を参照することにより利用者は、不正使用された状況を把握することが可能である。このように、自宅の利用者端末１００にも部分秘密鍵ＳＫｃを保管することにより、利用者は、部分秘密鍵の不正使用の検出、不正使用された状況の把握をすることが可能である。

【００７７】また、上記実施形態において、利用者端末１００における通信部１１０に利用者が携帯する携帯電話へ通信する機能を設け、利用者端末１００にアクセスがある毎に携帯電話に発信または、電子メールを利用者に送信するようにしてもよい。これにより、利用者は、利用者端末１００へのアクセス状況を把握できるので、予期しないアクセスをより早期に発見することが可能である。

【００７８】また、上記実施形態において、利用者端末１００に部分秘密鍵を保管し、アクセスするようにしたが、利用者の部分秘密鍵を保管する共同センタ端末を設け、この共同センタ端末に部分秘密鍵を保管し、店舗端末３００からのアクセスを受けるようにしてもよい。

【００７９】また、上記実施形態において、利用者端末１００にパスワードを設定し、店舗端末３００からのアクセス時において、入力されるパスワードが一致しない場合に、利用者端末１００にアクセスできないようにしてもよい。これにより、利用者端末１００に不正にアクセスすることを防止することができる。

【００８０】次に、部分秘密鍵の更新について図１１の構成における電子署名システムを例として図１３を用いて説明する。図１３は、部分秘密鍵の更新を行う動作について説明するためのフローチャートである。まず、利用者端末１００において、制御部１３１は、部分秘密鍵ＳＫａと部分秘密鍵ＳＫｃとを記憶部１１０から読み出

し（ステップＳ４０１）、一時保持する。次に、制御部１３１は、乱数生成部１８０によって乱数ａを生成させ、生成された乱数ａを取得し、一時保持する（ステップＳ４０２）。次に、制御部１３１は、以下に示す（１１）式と（１２）式に基づいて、新たな部分秘密鍵ＳＫａ´、部分秘密鍵ＳＫｃ´を生成する。

ＳＫａ´＝ＳＫａ＋ａ　……（１１）

ＳＫｃ´＝ＳＫｃ－ａ　……（１２）

制御部１３１は、生成された部分秘密鍵ＳＫａ´と部分秘密鍵ＳＫｃ´とを記憶部１１０に記憶するとともに、部分秘密鍵ＳＫａ´をＩＣカード５００の記憶部５３０に記憶する制御を行う。これにより、利用者端末１００の部分秘密鍵ＳＫａ´、ＩＣカード５００の部分秘密鍵ＳＫｃ´を更新することができる。

【００８１】上述した、ＩＣカードと利用者端末１００の部分秘密鍵の更新を行うことによって、ＩＣカードの紛失、盗難が発生した場合や、ＩＣカードの部分秘密鍵がコピーなどによってデータが持ち出された場合においても、ＩＣカードの部分秘密鍵を無効にすることができるので、ＩＣカードの停止をすることが可能である。また、利用者端末１００において部分秘密鍵の更新を行うことができるので、公開鍵明書を再取得したり、店舗に部分秘密鍵を再登録する手間を省くことができる。

【００８２】また、図１における処理部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより施工管理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピー（登録商標）ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【００８３】

【発明の効果】以上説明したように、この発明によれば、電子署名を生成するための鍵情報を分割し、ＩＣカードと店舗端末に記憶するようにしたので、分割した部分鍵情報を有しない店舗においては、電子署名を生成することができないので、ＩＣカードの使用できる店舗を限定でき、秘密鍵の紛失、盗難、盗聴などが発生した場合においても、悪意ある第三者によって秘密鍵が悪用される可能性を低減させることができ、鍵情報の機密性を向上できる効果が得られる。

【００８４】また、この発明によれば、鍵情報を分割して部分鍵情報を生成し、一度分割した部分鍵情報をさらに分割して各店舗端末に送信し、一度分割された部分鍵情報と二度分割された部分鍵情報の一部とをＩＣカードに記憶するようにしたので、使用先となる店舗同士が結託し、部分鍵情報を用いて署名を作成する、部分鍵情報を流用するといった使用先の不正使用を防止することができる効果が得られる。

【００８５】また、この発明によれば、メッセージに使用先コードを付加して部分署名を生成し、これらの部分署名を集めて電子署名を生成するようにしたので、ＩＣカードの利用者は、部分鍵情報の送信となる店舗でしか生成できないメッセージに対して電子署名を行うことが可能である。従って、第三者によって電子署名が設定されたメッセージの契約書内の契約先の名称が、利用者が実際には契約を行っていない場合の契約先の名称に改竄された場合、改竄された契約先名称とメッセージに予め設定されている契約先の名称とが異なるので、改竄を発見することが可能であり、電子署名を部分鍵情報の預け先以外に流用されることを防ぐことが可能である。

【図面の簡単な説明】

【図１】　この発明の一実施形態による電子署名システムの構成を示す概略ブロック図である。

【図２】　シークレットシェアを説明するための概念図である。

【図３】　図１の構成における電子署名システムの動作について説明するためのフローチャートである。

【図４】　第２の実施形態における電子署名システムの構成を示す概略ブロック図である。

【図５】　図４の構成における電子署名システムの動作について説明するためのフローチャートである。

【図６】　第３の実施形態における電子署名システムの構成を示す概略ブロック図である。

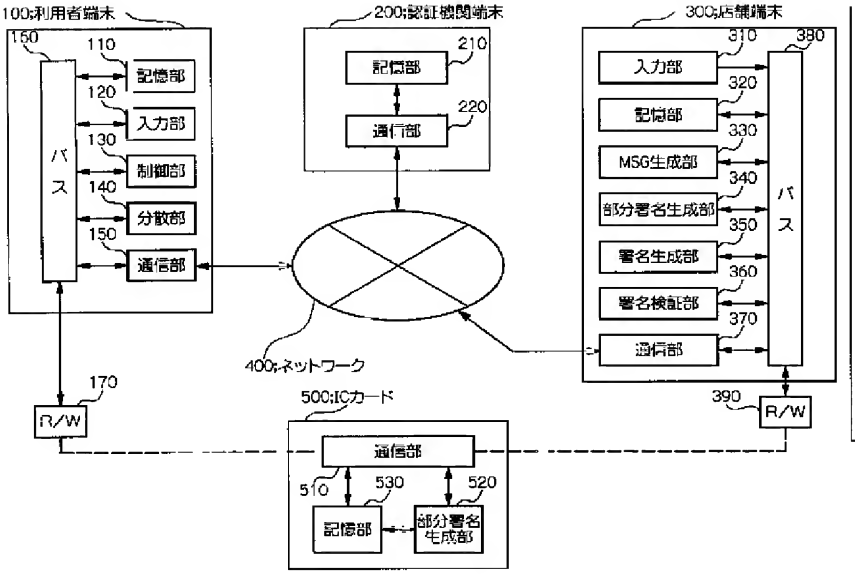
【図７】　図６の構成における装置の動作について説明するためのフローチャートである。

【図８】　部分秘密鍵ＳＫａ、部分秘密鍵ＳＫｂｉをＩＣカード５００、店舗端末３００に設定する動作を説明するためのフローチャートである。

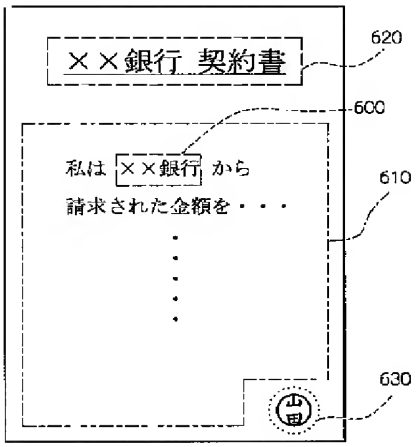
【図９】　第４の実施形態における電子署名システムの構成を示す概略ブロック図である。

【図１０】　使用先コードＩＤｉがＭｓｇ内に設定された状態を説明するための概念図である。
【図１１】　第５の実施形態における電子署名システムの構成について説明するための概略ブロック図である。
【図１２】　図１１の構成における装置の動作について説明するためのフローチャートである。
【図１３】　部分秘密鍵の更新を行う動作について説明するためのフローチャートである。
【符号の説明】
１００　利用者端末、　１１０　記憶部、　１３０、１３１　制御部、１４０、１４１　分散部、　１５０　通信部、　１８０　乱数生成部、１９０　部分秘密鍵演算部、　１９５　部分署名生成部、３００　店舗端末、　３２０　記憶部、　３３０　ＭＳＧ生成部、３４０、３４１　部分署名生成部、　３５０、３５１　署名生成部、３７０　通信部、　５００　ＩＣカード、５２０、５２１　部分署名生成部、　５３０　記憶部、５４０　署名生成部、　５５０　部分秘密鍵生成部

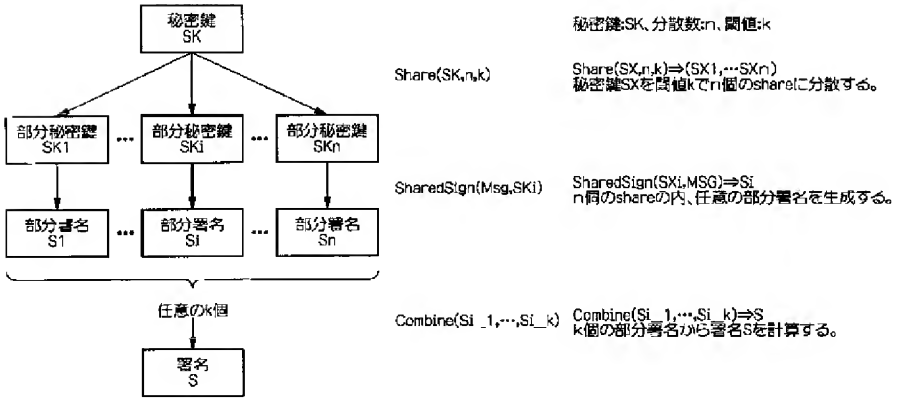
【図１】



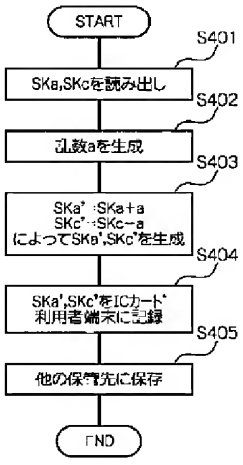
【図１０】



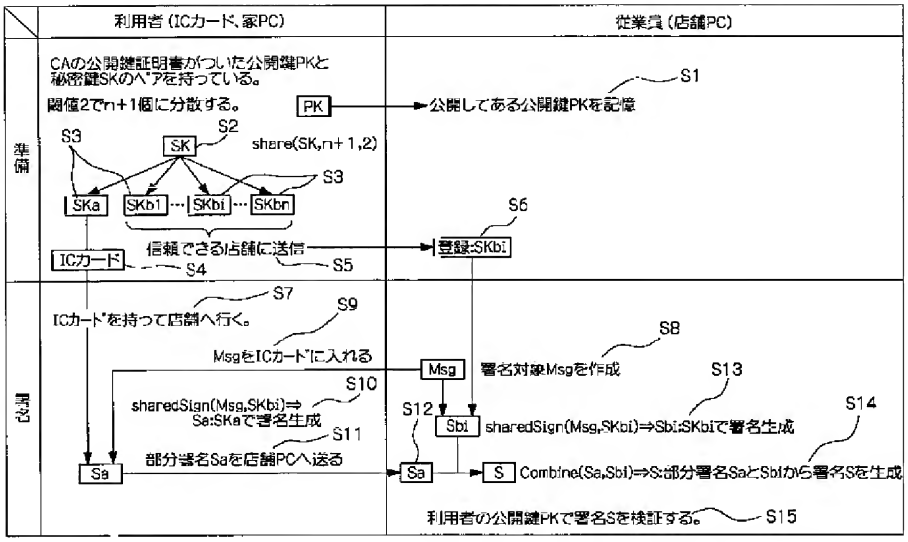
【図２】



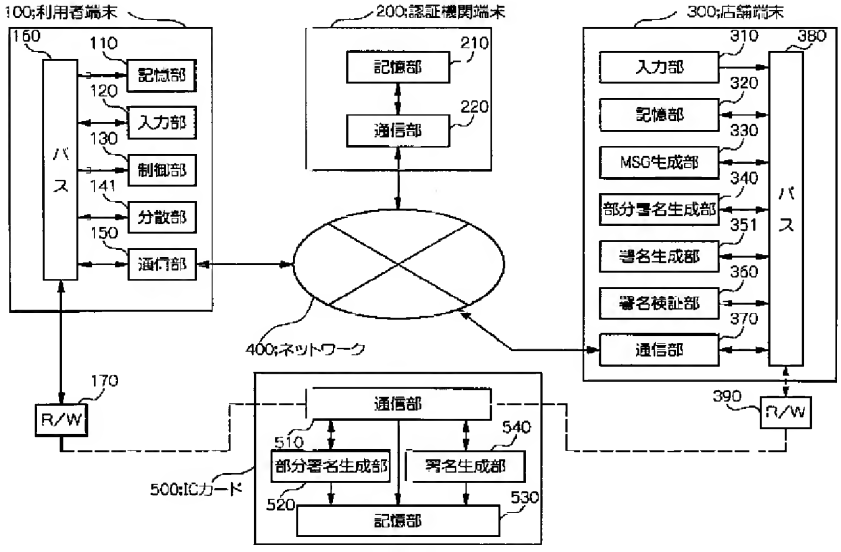
【図１３】



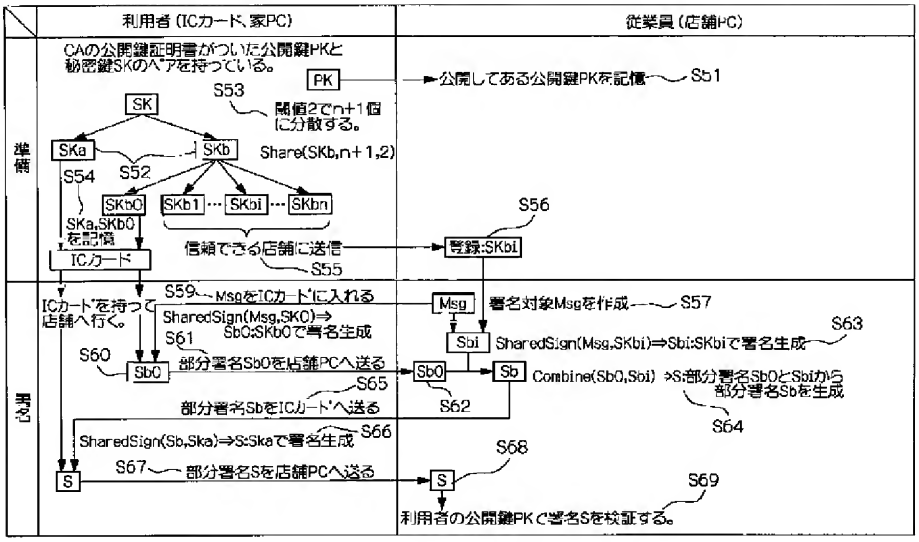
【図３】


利用者（ICカード、家PC）
従業員（店舗PC）
準備
CAの公開鍵証明書がついた公開鍵PKと
秘密鍵SKのペアを持っている。
閾値2でn+1個に分散する。
PK
公開してある公開鍵PKを記憶
S1
S2
SK
share(SK,n+1,2)
S3
SKa
SKb1
SKbi
SKbn
S6
登録:SKbi
ICカード
信頼できる店舗に送信
S4
S5
購入
S7
ICカードを持って店舗へ行く。
S9
MsgをICカードに入れる
S8
Msg
署名対象Msgを作成
S13
S10
sharedSign(Msg,SKbi)⇒
Sa:SKaで署名生成
S12
Sbi
sharedSign(Msg,SKbi)⇒Sbi:SKbiで署名生成
S14
S11
部分署名Saを店舗PCへ送る
Sa
Sa
S
Combine(Sa,Sbi)⇒S:部分署名SaとSbiから署名Sを生成
利用者の公開鍵PKで署名Sを検証する。
S15

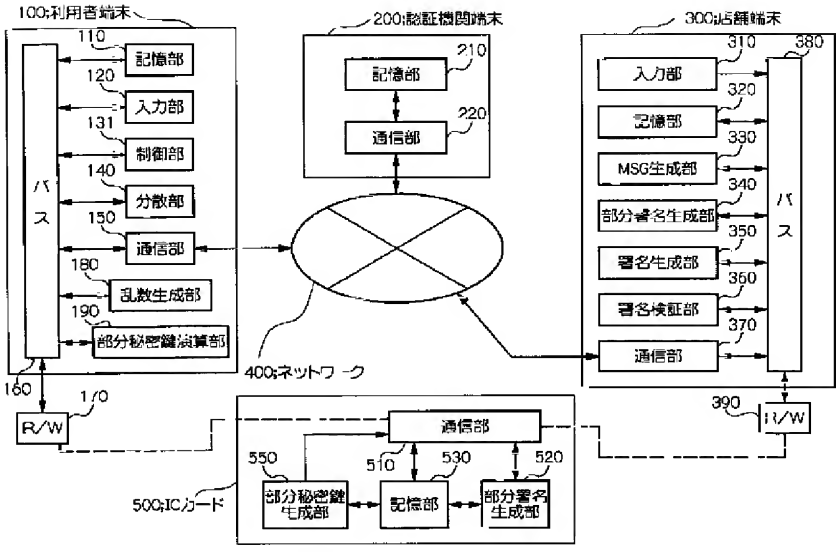
【図４】


100:利用者端末
150
110
記憶部
120
入力部
130
制御部
141
分散部
150
通信部
バス
200:認証機関端末
210
記憶部
220
通信部
300:店舗端末
310
入力部
320
記憶部
330
MSG生成部
340
部分署名生成部
351
署名生成部
350
署名検証部
370
通信部
380
バス
400:ネットワーク
170
R/W
390
R/W
500:ICカード
510
通信部
部分署名生成部
540
署名生成部
520
記憶部
530

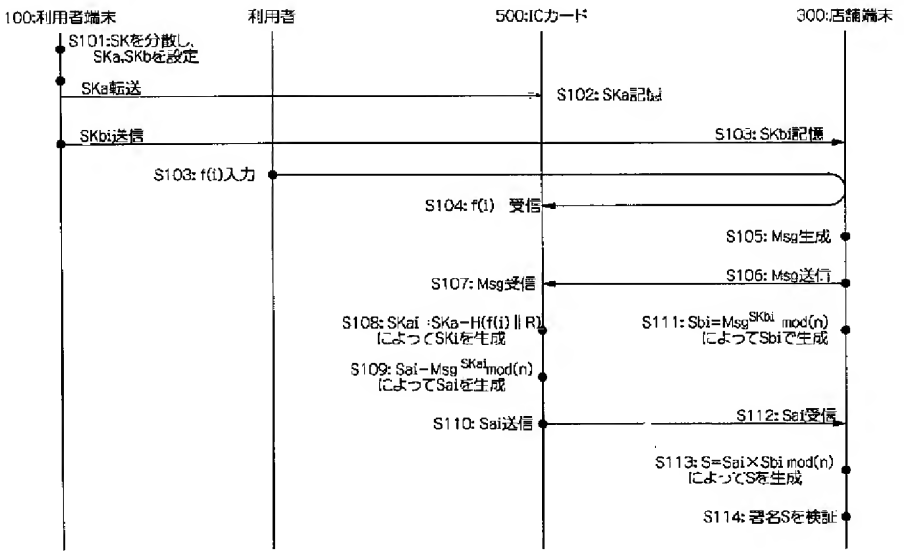
【図5】


利用者（ICカード、家PC）
従業員（店舗PC）
準備
処理
CAの公開鍵証明書がついた公開鍵PKと
秘密鍵SKのペアを持っている。
PK
公開してある公開鍵PKを記憶
S51
S53
SK
閾値2でn+1個
に分散する。
SKa
SKb
Share(SKb,n+1,2)
S54
S52
SKb0
SKb1
SKbi
SKbn
SKa,SKb0
を記憶
ICカード
信頼できる店舗に送信
S55
S56
登録:SKbi
S59
Msgを ICカードに入れる
ICカードを持って
店舗へ行く。
SharedSign(Msg,SKC)⇒
Sb0:SKb0で署名生成
S61
S60
Sb0
部分署名Sb0を店舗PCへ送る
S65
部分署名Sbを ICカードへ送る
S66
SharedSign(Sb,Ska)⇒S:Skaで署名生成
S67
部分署名Sを店舗PCへ送る
S
Msg
署名対象Msgを作成
S57
Sbi
SharedSign(Msg,SKbi)⇒Sbi:SKbiで署名生成
S63
Sb0
Sb
Combine(Sb0,Sbi) ⇒S:部分署名Sb0とSbiから
部分署名Sbを生成
S62
S64
S68
S
S69
利用者の公開鍵PKで署名Sを検証する。

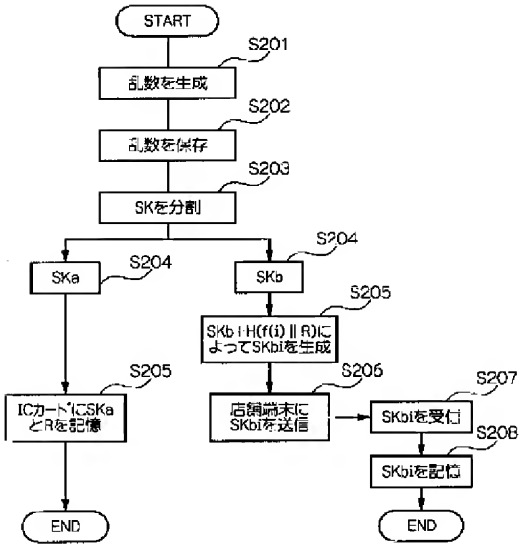
【図6】


100:利用者端末
110
記憶部
120
入力部
131
制御部
140
分散部
150
通信部
180
乱数生成部
190
部分秘密鍵演算部
バス
160
R/W
I/O
200:認証機関端末
210
記憶部
220
通信部
400:ネットワーク
300:店舗端末
310
入力部
320
記憶部
330
MSG生成部
340
部分署名生成部
350
署名生成部
360
署名検証部
370
通信部
380
バス
390
I/W
500:ICカード
通信部
550
510
530
520
部分秘密鍵
生成部
記憶部
部分署名
生成部

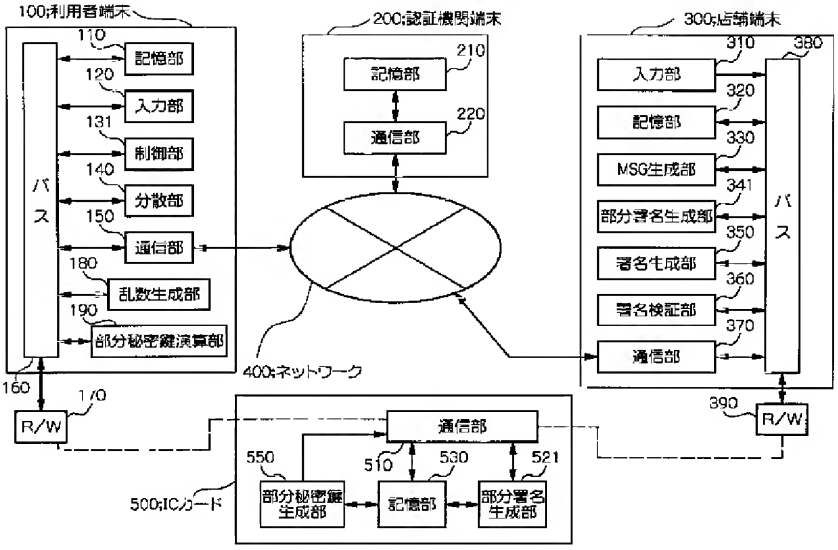
【図7】


100:利用者端末
利用者
500:ICカード
300:店舗端末
S101:SKを分散し、SKa,SKbを設定
SKa転送
S102: SKa記憶
SKbi送信
S103: SKbi記憶
S103: f(i)入力
S104: f(i) 受信
S105: Msg生成
S107: Msg受信
S106: Msg送信
S108: SKai :SKa−H(f(i)‖R)によってSKiを生成
S111: Sbi=Msg^SKbi mod(n)によってSbiで生成
S109: Sai−Msg^SKai mod(n)によってSaiを生成
S110: Sai送信
S112: Sai受信
S113: S=Sai×Sbi mod(n)によってSを生成
S114: 署名Sを検証

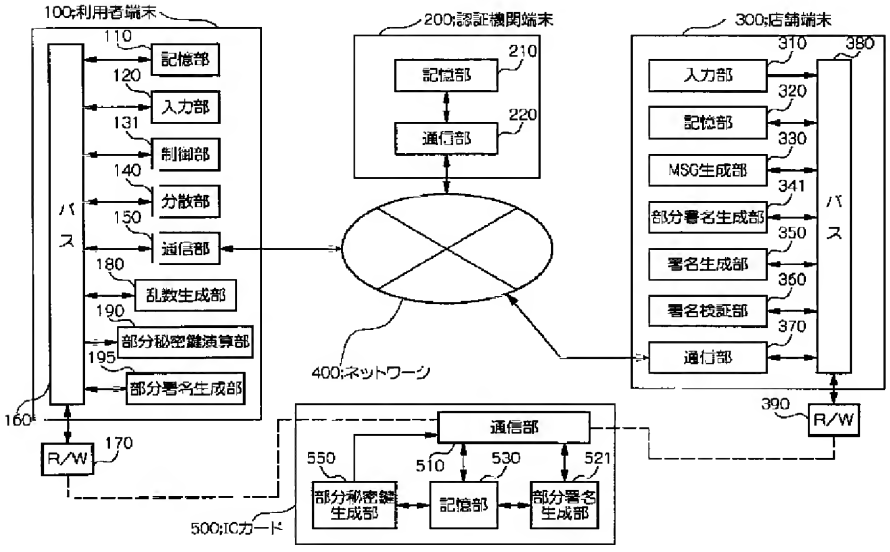
【図8】


START
S201
乱数を生成
S202
乱数を保存
S203
SKを分割
S204
SKa
S204
SKb
S205
SKb:H(f(i)‖R)によってSKbiを生成
S205
ICカードにSKaとRを記憶
S206
店舗端末にSKbiを送信
S207
SKbiを受信
S208
SKbiを記憶
END
END

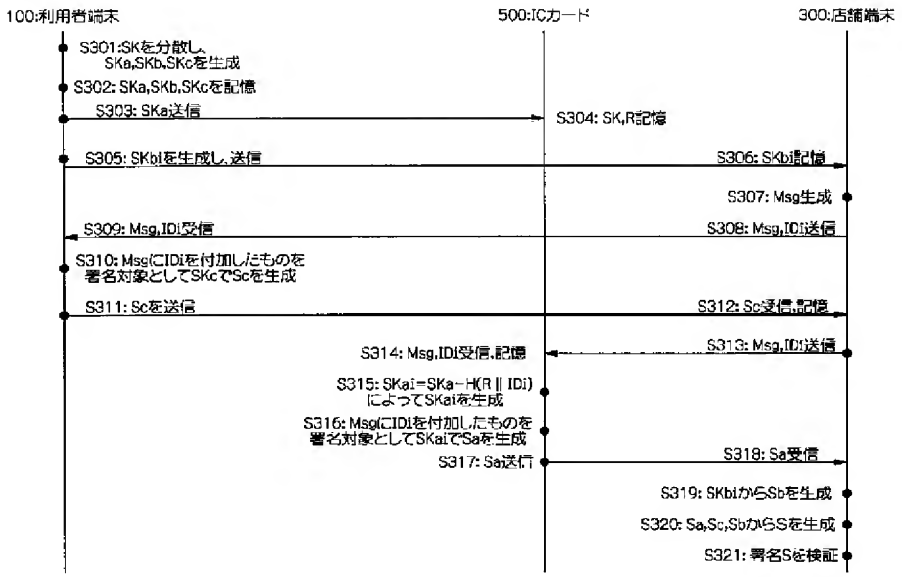
【図9】


100;利用者端末
110
記憶部
120
入力部
131
制御部
140
分散部
150
通信部
180
乱数生成部
190
部分秘密鍵演算部
バス
160
R/W
170
200;認証機関端末
210
記憶部
220
通信部
400;ネットワーク
300;店舗端末
310
入力部
320
記憶部
330
MSG生成部
341
部分署名生成部
350
署名生成部
360
署名検証部
370
通信部
380
バス
390
R/W
500;ICカード
通信部
550
510
530
521
部分秘密鍵生成部
記憶部
部分署名生成部

【図11】


100;利用者端末
110
記憶部
120
入力部
131
制御部
140
分散部
150
通信部
180
乱数生成部
190
部分秘密鍵演算部
195
部分署名生成部
バス
160
R/W
170
200;認証機関端末
210
記憶部
220
通信部
400;ネットワーク
300;店舗端末
310
入力部
320
記憶部
330
MSG生成部
341
部分署名生成部
350
署名生成部
360
署名検証部
370
通信部
380
バス
390
R/W
500;ICカード
通信部
550
510
530
521
部分秘密鍵生成部
記憶部
部分署名生成部

【図12】


100:利用者端末
500:ICカード
300:店舗端末
S301:SKを分散し、SKa,SKb,SKcを生成
S302: SKa,SKb,SKcを記憶
S303: SKai送信
S304: SK,R記憶
S305: SKbiを生成し、送信
S306: SKbi記憶
S307: Msg生成
S308: Msg,IDi送信
S309: Msg,IDi受信
S310: Msg(にIDiを付加したものを署名対象としてSKcでScを生成
S311: Scを送信
S312: Sc受信,記憶
S313: Msg,IDi送信
S314: Msg,IDi受信,記憶
S315: SKai=SKa−H(R‖IDi)によってSKaiを生成
S316: Msg(にIDiを付加したものを署名対象としてSKaiでSaを生成
S317: Sai送信
S318: Sa受信
S319: SKbiからSbを生成
S320: Sa,Sc,SbからSを生成
S321: 署名Sを検証